UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

MICROSOFT CORPORATION, a Washington Corporation, Plaintiff, v. JOHN DOES 1-10 using IP addresses 64.173.244.84 and 64.173.244.85, Defendants.	CASE NO. C17-0688RSM ORDER GRANTING PLAINTIFF'S MOTION TO EXPEDITE DISCOVERY

I. INTRODUCTION

Plaintiff alleges copyright and trademark infringement claims against several unknown John Doe Defendants that appear to be using IP addresses 64.173.244.84 and 64.173.244.85 to illegally activate Plaintiff's software. Dkt. #1 at ¶ ¶ 44-57. It now seeks permission to take limited, expedited discovery from AT&T Services, Inc. ("AT&T"), an internet service provider ("ISP"), to identify and name the John Doe Defendants in this case so that it can complete service of process and proceed with litigation. Dkt. #9 at 6-7. As further discussed below, Plaintiff has demonstrated that: (1) the John Doe Defendants are real people and/or entities that

may be sued in federal court; (2) it has unsuccessfully attempted to identify the John Doe Defendants prior to filing this motion; (3) its claims against the John Doe Defendants would likely survive a motion to dismiss; and (4) there is a reasonable likelihood that service of the proposed subpoena on AT&T will lead to information identifying the John Doe Defendants. As a result, the Court finds that good cause exists to allow Microsoft to engage in expedited, preliminary discovery.

II. BACKGROUND[1]

Plaintiff develops, distributes, and licenses various types of computer software, including operating system software (such as Microsoft Windows) and productivity software (such as Microsoft Office). Dkt. #1 at ¶ ¶ 11–21. Microsoft holds registered copyrights in the various different versions of these products, and has registered trademarks and service marks associated with the products. *Id.* ¶ 22.

Microsoft has implemented a wide-range of initiatives to protect its customers and combat theft of its intellectual property, including its product activation system, which involves the activation of software through product keys. *Id.* ¶ 30. A Microsoft product key is a 25-character alphanumeric string generated by Microsoft and provided either directly to Microsoft's customers or to Microsoft's original equipment manufacturer ("OEM") partners. *Id.* ¶ 31. Generally, when customers or OEMs install Microsoft software on a device, they must enter the product key. *Id.* Then, as part of the activation process, customers and/or OEMs voluntarily contact Microsoft's activation servers over the Internet and transmit the product keys and other technical information about their device to the servers. *Id.* Because Microsoft software is capable of being installed on an unlimited number of devices, Microsoft

[1] The following background is taken from Plaintiff's Complaint and the Declaration of Brittany Carmichael filed in support of Plaintiff's Motion for Expedited Discovery. Dkts. #1 and #10.

uses the product activation process to detect piracy and protect consumers from the risk of non-genuine software. *Id.* ¶ 32.

Microsoft has created the Microsoft Cybercrime Center where they utilize, *inter alia*, certain technology to detect software piracy, which it refers to as "cyberforensics." *Id.* at ¶ 35. Microsoft uses its cyberforensics to analyze product key activation data voluntarily provided by users when they activate Microsoft software, including the IP address from which a given product key is activated. Dkt. #1 at ¶ 36. Cyberforensics allows Microsoft to analyze the activations of Microsoft software and identify activation patterns and characteristics that make it more likely than not that the IP address associated with certain product key activations is one through which unauthorized copies of Microsoft software are being activated. Dkt. #10 at ¶ ¶ 2-5. Microsoft's cyberforensics have identified a number of product key activations originating from IP addresses 64.173.244.84 and 64.173.244.85. *Id.* at ¶ 6. According to publicly available data, those IP addresses are presently under the control of AT&T. *Id.*

Microsoft alleges that for at least the past three years, the aforementioned IP addresses have been used to activate hundreds of Microsoft product keys. *Id.* at ¶ 7. These activations have characteristics that demonstrate that the John Doe Defendants are using the IP addresses to activate unauthorized copies of Microsoft's software. *Id*. Microsoft believes these activations constitute the unauthorized copying, distribution, and use of Microsoft software, in violation of Microsoft's software licenses and intellectual property rights. *Id*. at ¶ 8. Despite its efforts, Microsoft has been unable to positively identify the John Doe Defendants. *Id.* at ¶ 9. Microsoft believes AT&T has access to the subscriber information associated with the IP addresses from records kept in the regular course of its business. *Id.* at ¶ 11.

III. DISCUSSION

A. Legal Standard

This Court may authorize early discovery before the Rule 26(f) conference for the parties' and witnesses' convenience and in the interests of justice. Fed. R. Civ. P. 26(d). Courts within the Ninth Circuit generally consider whether a plaintiff has shown "good cause" for such early discovery. *See, e.g., Yokohama Tire Crop. v. Dealers Tire Supply, Inc.*, 202 F.R.D. 612, 613-14 (D. Ariz. 2001) (collecting cases and standards). When the identities of defendants are not known before a Complaint is filed, a plaintiff "should be given an opportunity through discovery to identify the unknown defendants, unless it is clear that discovery would not uncover the identities, or that the complaint would be dismissed on other grounds." *Gillespie v. Civiletti*, 629 F.2d 637, 642 (9th Cir. 1980). In evaluating whether a plaintiff establishes good cause to learn the identity of John Doe defendants through early discovery, courts examine whether the plaintiff (1) identifies the John Doe defendant with sufficient specificity that the Court can determine that the defendant is a real person who can be sued in federal court, (2) recounts the steps taken to locate and identify the defendant, (3) demonstrates that the action can withstand a motion to dismiss, and (4) proves that the discovery is likely to lead to identifying information that will permit service of process. *Columbia Ins. Co. v. seescandy.com*, 185 F.R.D. 573, 578-80 (N.D. Cal. 1999).

B. Plaintiff Has Shown Good Cause to Take Early Discovery

Here, Plaintiff established good cause to engage in early discovery to identify the John Doe Defendants. First, Plaintiff has associated the John Doe Defendants with specific acts of activating unauthorized software using product keys that are known to have been stolen from Microsoft, and have been used more times than are authorized for the particular software. Dkt.

#10 at ¶ ¶ 6-8. Plaintiff has been able to trace the product key activations as originating from two IP addresses, and nearly all of the activations have involved voluntary communication between the John Doe Defendants and Microsoft activation servers in this judicial District. *Id.* at ¶ 7. Second, Plaintiff has adequately described the steps it took in an effort to locate and identify the John Doe Defendants. Dkt. #10. Specifically, it utilized its "cyberforensics" technology to analyze product key activation data and identified certain patterns and characteristics which indicate software piracy. Dkt. #10 at ¶ ¶ 2-4 and Dkt. #1 at ¶ ¶ 35-38. Third, Plaintiff has pleaded the essential elements to state a claim for Copyright Infringement under 17 U.S.C. § 501, *et seq.*, and Trademark Infringement under 15 U.S.C. § 1114. Dkt. #1 at ¶ ¶ 44-57 and Exs. 1-51. Fourth, the information proposed to be sought through a Rule 45 subpoena appears likely to lead to identifying information that will allow Plaintiff to effect service of process on the John Doe Defendants. Dkt. #10 at 11-12. Specifically, Plaintiff states it will seek subscriber information associated with the alleged infringing IP addresses. Dkt. #10 at ¶ 12.

Taken together, the Court finds that the foregoing factors demonstrate good cause to grant Plaintiff's motion for leave to conduct limited expedited discovery. *See Semitool*, 208 F.R.D. at 276. Therefore, the Court will grant discovery limited to documents and/or information that will allow Plaintiff to determine the identities of the John Doe Defendants in order to effect service of process.

///

///

///

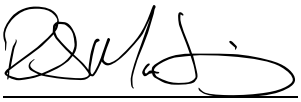
///

IV. CONCLUSION

For the reasons set forth above, the Court hereby ORDERS:

1. Plaintiff may immediately serve on AT&T Services, Inc. (or its associated downstream ISPs) a Rule 45 subpoena to obtain documents and/or information to identify John Does 1-10.
2. At this time, any document requests shall be limited to documents sufficient to identify all names, physical addresses, PO boxes, electronic addresses (including email addresses), telephone numbers, or other customer identifying information that are or have been associated with the IP addresses 64.173.244.84 and 64.173.244.85.

DATED this 30 day of May, 2017.



RICARDO S. MARTINEZ
CHIEF UNITED STATES DISTRICT JUDGE